TOWARDS AN INFERENTIALIST METAPHYSICS OF INFORMATION SECURITY THROUGH PROOF-THEORETIC SEMANTICS (EXTENDED ABSTRACT)

MATTHEW COLLINSON*, TIMO ECKHARDT*, AND DAVID PYM*

1. What is information security?

The idea of security is very old — hidden caches of resources, coded messages, locked doors, and safes with combination locks are all examples of the idea. Partly as a result of this longevity, there are in circulation many 'definitions' of information security, too numerous to discuss in detail here. Mostly, they are of limited value, being confused or being too closely related to a particular perspective. One example is, 'the state of being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this'. Another is, 'the protection of information and information systems from unauthorized access and disruption'. Among other issues, these attempts introduce the terms 'protection', 'unauthorized', and 'disruption', all of which themselves require definition and which, since they are in use in the field of security, introduce a degree of confusion. This is all rather uninspiring.

A more useful working definition of information security, with more conceptual clarity, goes as follows: *Information security is the process of ensuring that just the right agents have just the right access to just the right information at just the right times.* This is a rather dense and slightly abstract definition, the components of which it is useful to analyse. It at least avoids many of the weaknesses of many of the definitions that are in circulation.

The first, and perhaps most critical observation, is that this, and indeed any, definition of security must be understood as being about *systems* and *agency*. In terms of the analyses of Dretske [15, 16] and van Benthem [34, 32, 33], we are now addressing the metaphysics of information.

2. Dretske and van Benthem on information and agency

We start from Dretske's account of the metaphysics of information [15, 16]. It identifies three key properties of information: intentionality, truth, and transmissibility.

Intentionality states that information has to be about something and has to be understood as a semantic object; that is, that is, the content (what is conveyed) rather than the vehicle (the signal used to send it). *Truth* requires information to be correct because of its epistemological role as a necessary condition for knowledge. *Transmissibility* conveys that information must be sent and received in such a way that the agent receiving the information can absorb it and so acquire knowledge. We adapt Dretske's framework with an inferentialist version in which truth is replaced by inferability.

Inferentialism [7, 8, 21] is, essentially, the philosophical position that the meaning of linguistic constructs, including the expressions of formal logic, is determined by their use. A mathematical logical realization of this position is offered by proof-theoretic semantics, which offers theories of validity for both formulae and proofs that are grounded in a primitive notion of inference. These are two strains of proof-theoretic semantics: theories of validity for proofs sometimes called proof-theoretic validity (P-tV) (e.g., [24, 17, 18, 29, 20]) and theories of validity of formulae called base-extension semantics (B-eS) (e.g., [27, 28]). Here we are concerned with B-eS. In B-eS, the meaning of atomic formulae relative to a base of inference rules is given in terms of provability given those inference rules. The logical connectives are inductively defined as usual. This means that the validity of formulae is inherently based in inference rather than given by abstract mathematical objects like, for example, valuations in Kripke semantics.

We argue that an inferentialist view of reasoning is appropriate for information, and especially for information security, because it offers directly traceable evidence for the conclusions that it supports. A conclusion supported by a system can be traced back to the premisses and rules used

*Corresponding author. The authors thank Tim Button for his comments on a draft of this extended abstract.

to infer it, so allowing us to identify the provenance of pieces of information that are relevant to the security of the system.

Among logical theories, van Benthem and Martinez [35] identify three categories: Information-as-range models information by the range of possibilities that are consistent with it (e.g., epistemic logics), information-as-correlation treats information as existing in different situations with dependencies between them (e.g., situation theory [4, 13, 14, 5, 1]), and information-as-code treats information as being encoded in sentences and messages (e.g., Shannon's work [30]).

We draw heavily on situation theory. Situation theory defines so-called 'infons' as the basic building blocks of information and uses them to define (abstract) situations as sets of such infons. This allows for a theory on how pieces of information are constructed and, by making locations explicit, allows for modelling of information flow between 'source' and 'target' locations.

In [10], we reconstructed the ideas of situation theory using the tools of proof-theoretic semantics underpinned by an inferentialist variation of Dretske's metaphysics in which the characteristic of truth is replaced by a characteristic of inferential validity (see Section 4). As in situation theory, this logical framework treats information as correlation. In such an inferentialist account, information is understood in light of the inferences it enables. The informational content of, say, a message is defined by the inferences that are possible after receiving it that were not possible before. This will provide the basis for our logical framework to information security.

We address a shortcoming of that account: A notion implicit there, and also in Dretske's metaphysics, is that of agents. As Martinez and van Benthem in [35] point out, there is an interplay between the available information at a situation and the powers of the agents that have access to it. This becomes especially important in the information security context, as it becomes important to track who has access to certain information and, for example, whether they might have tampered with it. We make agency explicit here by adding methods from epistemic logic to our framework allowing us to treat the information agents have access to separately from all available information. This results in a logical theory of both information-as-correlation and information-as-range.

3. Adding the concepts of information security

Starting from our inferentialist variation of Dretske's account of information, a metaphysics of information security requires incorporating the security concepts. As we discussed, these concepts are only meaningful in the context of a concept of system that includes a concept of agency [34].

The first key observation is that information security is not a state, but rather a process: a security property may hold today, but not necessarily tomorrow — the threat environment may have changed, so the security posture may need to evolve. This imposes a requirement that we must have a concept of system that incorporates evolution.

Concepts such as *confidentiality*, *integrity*, and *availability* are, for a given system, *declarative* objectives. For example, the system's operators might require that only specified agents may access specified resources, that the state of the system as of the previous day must be recoverable, or that the system be capable of operating normally 99.99% of the time. The operators deploy *operational* tools to deliver their declarative objectives. For example, authorization and authentication tools control which agents have what access, redundant back-ups ensure previous system states can be recovered, and multiple distributed servers ensure high levels of availability. Other declarative properties of interest might be concerned with the *sustainability* and *resilience* of the system and its policies [25]. Some of these ideas are considered through inferentialist logic in [19, 10].

4. Inferonics and its extension to information security

We give a very brief summary of our proposed logical set-up for delivering a formal metaphysics of information security. We begin with an extremely brief summary of a proof-theoretic semantics for intuitionistic propositional logic (IPL) and then explain (following [10]) how we can incorporate a primitive unit of information, the *inferon*, which is an inferentialist counterpart to the concept of 'infon' introduced by Barwise et al. in situation theory (e.g., [4, 3, 13, 5]).

B-eS for IPL. Sandqvist [27] gives a base-extension semantics for IPL for which natural deduction in the system NJ is sound and complete. A base $\mathcal{B}$ is a set of atomic rules (for $\vdash_{\mathcal{B}}$) as in Definition 1, which also defines the application of base rules, and validity in a base ($\Vdash_{\mathcal{B}}$). Roman p, P, etc. denote atoms and sets of atoms; Greek ϕ, Γ, etc. denote formulae and sets of formulae.

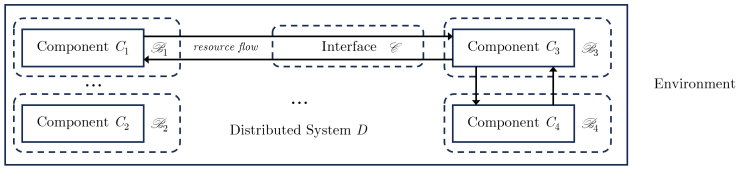

FIGURE 1. A generic distributed system (adapted from [19], cf. [22])

Definition 1 (Sandqvist's Semantics)**.** Base rules $\mathcal{R}$, application of base rules, and *validity* of formulae in a (possibly finite) countable base $\mathcal{B}$ of rules $\mathcal{R}$ are defined as follows:

$$\frac{\begin{array}{ccc}[P_1] & & [P_n] \\ q_1 & \dots & q_n\end{array}}{r}\,\mathcal{R}$$

(Ref) $P, p \vdash_{\mathcal{B}} p$

($\text{App}_{\mathcal{R}}$) if $((P_1 \Rightarrow q_1), \dots, (P_n \Rightarrow q_n)) \Rightarrow r)$ and, for all $i \in [1, n]$, $P, P_i \vdash_{\mathcal{B}} q_i$, then $P \vdash_{\mathcal{B}} r$

(At) for atomic p, $\Vdash_{\mathcal{B}} p$ iff $\vdash_{\mathcal{B}} p$

($\vee$) $\Vdash_{\mathcal{B}} \phi \vee \psi$ iff, for every atomic p and every $\mathcal{C} \supseteq \mathcal{B}$, if $\phi \Vdash_{\mathcal{C}} p$ and $\psi \Vdash_{\mathcal{C}} p$, then $\Vdash_{\mathcal{C}} p$

($\supset$) $\Vdash_{\mathcal{B}} \phi \supset \psi$ iff $\phi \Vdash_{\mathcal{B}} \psi$

($\bot$) $\Vdash_{\mathcal{B}} \bot$ iff, for all atomic p, $\Vdash_{\mathcal{B}} p$

($\wedge$) $\Vdash_{\mathcal{B}} \phi \wedge \psi$ iff $\Vdash_{\mathcal{B}} \phi$ and $\Vdash_{\mathcal{B}} \psi$

(Inf) for $\Theta \neq \emptyset$, $\Theta \Vdash_{\mathcal{B}} \phi$ iff, for every $\mathcal{C} \supseteq \mathcal{B}$, if $\Vdash_{\mathcal{C}} \theta$ for every $\theta \in \Theta$, then $\Vdash_{\mathcal{C}} \phi$ □

Theorem 2 (Soundness & Completeness)**.** Define (cf. [27]) $\Gamma \Vdash \phi$ as: for all $\mathcal{B}$, if $\Vdash_{\mathcal{B}} \psi$ for all $\psi \in \Gamma$, then $\Vdash_{\mathcal{B}} \phi$. Then $\Gamma \vdash \phi$ (in natural deduction for IPL, cf. [27]) iff $\Gamma \Vdash \phi$. □

Inferons. The infons of situation theory are grounded in model-theoretic semantics, with their meaning being given by a relation symbol. By contrast, inferons are grounded in base-extension semantics, with meaning deriving from provability in a base [10]:

$$\text{(At)} \quad \Vdash_{\mathcal{B}} \langle\!\langle P, \mathcal{P}, \mathfrak{b} \rangle\!\rangle \quad \text{iff} \quad \vdash_{\mathcal{B} \cup \mathcal{P}} \langle\!\langle P, \mathfrak{b} \rangle\!\rangle, \text{ for atomic propositions } P$$

We understand the base $\mathcal{B}$ as a model for the ambient system and the base $\mathcal{P}$ as being the specific inferences associated with the (atomic) propositional assertion P. As in situation theory, $\mathfrak{b}$ is a 'polarity'; cf. Rumfitt's assertion/denial [26]. We let ι, etc., denote (possibly compound) inferons.

Distributed systems and information flow. We have argued that the concepts of security make sense only in the context of systems, with agents. In informatics, a key idea is that of a *distributed system* [31, 12]. Mathematically, we abstract to the essential elements of a distributed system as follows: *locations*, *resources*, *processes*, and, critically, *environment/interfaces* (e.g., [11, 2, 9, 23, 32]. The essential idea is depicted in Figure 1, in which the components of a system reside at locations with bases that model their function.

Information flow and security. Security 'models', such as the celebrated 'Bell-LaPadula' confidentiality model [6] are really policies about information flow within systems. Bell-LaPadula (BLP) includes the 'simple confidentiality property': an agent [or 'subject'] at a given security level may not read an object at a higher security level. To see how we can analyse this policy, consider the system depicted in Figure 1 and suppose that the security level of C_1 is lower than that of C_3. BLP requires that an agent at C_1 may not read at C_2 and that an agent at C_2 may not write at C_1.

In the logic of inferons, we need to employ familiar-looking agent modalities

$$\Vdash_{\mathcal{C}} [a]\iota \quad \text{iff} \quad \text{for all } \mathcal{A} \in \mathbf{Bases}(a), \Vdash_{\mathcal{C} \cup \mathcal{A}} \iota \qquad \Vdash_{\mathcal{C}} \langle a \rangle \iota \quad \text{iff} \quad \text{for some } \mathcal{A} \in \mathbf{Bases}(a), \Vdash_{\mathcal{C} \cup \mathcal{A}} \iota$$

to express these requirements, where agents, a, come along with their own inferential capacity, a set of bases, $\mathbf{Bases}(a)$, which, when agents perform their actions (we conflate these here, for brevity), are added to the ambient inferential strength of the component. This inferential capacity allows agents who receive transmitted information to absorb it as knowledge, as discussed above. In the evident logical way, we can assert the possibility of 'writing up' and necessity of *not* 'writing down' (also a property of BLP). Note that different policies may apply to different agents because of their different intensional inferential capacity in combination with the ambient base, and that the inferentialist logic records that the system supports or not the actions, thereby offering explicit evidence for the compliance or non-compliance of the system with the security 'model'. In our picture, inferential validity might be validated by the 'interface' component.

References

[1] S. Abramsky and J. Väänänen, *From IF to BI*, Synthese, 167 (2009), pp. 207–230.

[2] G. Anderson and D.Pym, *A calculus and logic of bunched resources and processes*, Theoretical Computer Science, 614 (2016), pp. 63–96.

[3] J. Barwise and J. Etchemendy, *Information, infons, and inference*, in Situation Theory and Its Applications; Volume 1, Center for the Study of Language (CSLI), 1990, pp. 33–78.

[4] J. Barwise and J. Perry, *Situations and Attitudes*, MIT Press, Cambridge, MA, 1983.

[5] J. Barwise and J. Seligman, *Information Flow: The Logic of Distributed Systems*, Cambridge University Press, 1997.

[6] D. Bell and L. LaPadula, *Secure Computer Systems: Mathematical Foundations*. MITRE Technical Report 2547, Volume I. `https://web.archive.org/web/20060618092351/http://www.albany.edu/acc/courses/ia/classics/belllapadula1.pdf`, accessed 27 July 2026, 1973.

[7] R. Brandom, *Making It Explicit: Reasoning, Representing, and Discursive Commitment*, Harvard University Press, Cambridge, Mass., 1994.

[8] ———, *Articulating reasons: An introduction to inferentialism*, Harvard University Press, 2009.

[9] T. Caulfield, M.-C. Ilau, and D. Pym, *Engineering ecosystem models: Semantics and pragmatics*, in Simulation Tools and Techniques, D. Jiang and H. Song, eds., Cham, 2022, Springer International Publishing, pp. 236–258.

[10] M. Collinson, T. Eckhardt, and D. Pym, *Towards an Inferentialist Account of Information Through Proof-theoretic Semantics*. arXiv: `https://arxiv.org/abs/2605.05368`, 2026.

[11] M. Collinson, B. Q. Monahan, and D. J. Pym, *A Discipline of Mathematical Systems Modelling*, College Publications, 2012.

[12] G. Coulouris, J. Dollimore, T. Kindberg, and G. Blair, *Distributed Systems: Concepts and Design*, Addison-Wesley Publishing Company, USA, 5th ed., 2011.

[13] K. Devlin, *Logic and information*, Cambridge University Press, 1991.

[14] ———, *Situation theory and situation semantics*, in Logic and the Modalities in the Twentieth Century, D. M. Gabbay and J. Woods (editors), Handbook of the History of Logic, Volume 7, North-Holland, 2006, pp. 601–664.

[15] F. Dretske, *Knowledge and the Flow of Information*, The David Hume Series, CSLI Publications, 1999.

[16] ———, *The Metaphysics of Information*, in Wittgenstein and the Philosophy of Information, Alois Pichler and Herbert Hrachovec, ed., De Gruyter Brill, 2008, pp. 273–283.

[17] M. Dummett, *What is a theory of meaning?*, in Mind and language, S. D. Guttenplan, ed., Clarendon Press, 1975, pp. 97–138.

[18] ———, *The Logical Basis of Metaphysics*, Harvard University Press, 1991.

[19] A. Gheorghiu, T. Gu, and D. Pym, *Inferentialist Resource Semantics*, ENTICS 14727, 4 (Proceedings of MFPS XL) (2024). `https://doi.org/10.46298/entics.14727`.

[20] A. Gheorghiu and D. Pym, *From Proof-theoretic Validity to Base-extension Semantics for Intuitionistic Propositional Logic*, Studia Logica, (2025). `https://doi.org/10.1007/s11225-024-10163-9`.

[21] U. Hlobil and R. Brandom, *Reasons for Logic, Logic for Reasons: Pragmatics, Semantics, and Conceptual Roles*, Routledge, 2024.

[22] M.-C. Ilau, A. Baldwin, T. C. Caulfield, and D. Pym, *Modelling and simulating organizational ransomware recovery: structure, methodology, and decisions*, Journal of Cybersecurity, 11 (2025). `https://doi.org/10.1093/cybsec/tyaf035`.

[23] M.-C. Ilau, T. Caulfield, and D. Pym, *Interfaces in ecosystems: Concepts, form, and implementation.*, in Simulation Tools and Techniques. SIMUtools 2024. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, A. Juan, J. Guisado-Lizar, M. Morón-Fernández, and E. Perez-Bernabeu, eds., springer, 2025.

[24] D. Prawitz, *Ideas and Results in Proof Theory*, in Studies in Logic and the Foundations of Mathematics, vol. 63, Elsevier, 1971, pp. 235–307.

[25] D. Pym, *Category errors in (information) security: how logic can help*, Benthem's Gaze, (2015).

[26] I. Rumfitt, *"Yes" and "No"*, Mind, 109 (2000), p. 781–823.

[27] T. Sandqvist, *Base-extension semantics for intuitionistic sentential logic*, Logic Journal of the IGPL, 23 (2015), pp. 719–731.

[28] P. Schroeder-Heister, *Validity Concepts in Proof-Theoretic Semantics*, Synthese, 148 (2006), pp. 525–571.

[29] ———, *Proof-Theoretic versus Model-Theoretic Consequence*, in The Logica Yearbook 2007, M. Pelis, ed., Filosofia, 2008.

[30] C. E. Shannon, *A Mathematical Theory of Communication*, University of Illinois Press, 1949.

[31] A. S. Tanenbaum and M. V. Steen, *Distributed Systems: Principles and Paradigms*, Prentice Hall PTR, USA, 1st ed., 2001.

[32] J. van Benthem, *Logical Dynamics of Information and Interaction*, Cambridge University Press, 2011.

[33] ———, *Tracking Information*, Springer International Publishing, 2016, pp. 363–389.

[34] ———, *Logic, Information, and Agency*, CSLI Publications, The University of Chicago Press, 2025.

[35] J. van Benthem and M. Martinez, *The Stories of Logic and Information*, Handbook of the Philosophy of Information, Elsevier Science Publishers, Amsterdam, (2008), pp. 217–280. Commentators: Israel, David and Perry, John.

University of Aberdeen, King's College, Aberdeen AB24 3FX, Scotland, UK
Email address: matthew.collinson@aberdeen.ac.uk

UCL & Institute of Philosophy, University of London, Senate House, Malet Street, London WC1E 7HU, England, UK
Email address: t.echkhardt@ucl.ac.uk

UCL & Institute of Philosophy, University of London, Senate House, Malet Street, London WC1E 7HU, England, UK https://www.cantab.net/users/david.pym/
Email address: david.pym@sas.ac.uk